DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **3/15/11** has been entered.

Claims 99, 100, 106, and 111 have been cancelled. Claims 116 and 117 have been added. Claims 96-98, 101-105, 107-110, and 112-117 are pending.

Response to Arguments

Applicant's arguments with respect to claims 96 and 103 with respect to a public key certificate containing an electronic report pointer, the electronic record pointer being associated with each item of personal information of the registered user held in the electronic record system have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed 3/15/11 which respect to an anonymous public key certificate in a public key infrastructure have been fully considered but they are not persuasive. First in response to the allegation that Wheeler does not teach storing a private key within and under control of the portable storage device, this limitation is found in paragraph 107. To the notion that the devices are not associated with a register user it is noted that the devices and their internal keys are produced and earmarked at the time of manufacturing (0133). As stated before in the Final Rejection the claim is too broad to require a specific timing of performing the storing after a user has been registered. Earmarked devices at the time of manufacturing meet the claim's broad language.

Wheeler clearly teaches a public key infrastructure through the many embodiments. Wheeler specifically discloses public/private key pairs created and associated with devices and linking the devices and its users to a security record database (0131-0132). The claim language merely recites a “public key infrastructure” which clearly not distinguishable nor requires more than the system in which Wheeler employs his public keys.

Applicant alleges Wheeler does not teach a public key certificate. First of all in the art, a public key certificate is the public key signed and attested by a trusted entity. The certificate can have any number of content which may or may not identify the owner. However it must contain a public key and be signed by another party in order to be authenticated. Wheeler may not call his public key certificate by that name, but Fig. 7, and paragraph 0117 for example shows the creation of a pubic key certificate. The public keys are signed by the Secure Entity. One of ordinary skill in the art would appreciate this as the creation of a public key certificate. Moreover, the present amendments have necessitated a new reference which by the way also teaches public key certificates so the argued point is moot either way.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., de-identified personal information, another record system, independent of the device issuer) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The arguments presented rely heavily on what the Applicant believes are fundamental differences between the instant application and the cited prior art. If those differences have merit, they need to be incorporated into the claims to expressly recite those distinguishing features. For example, the arguments presented address the issue of anonymity contrasted between the instant application and cited prior. Applicant alleges there is no real anonymous certificate or anonymous framework in Wheeler because the database in no way anonymously indexed. As addressed in the previous Final Rejection, the claims' of the instant application merely recite anonymously indexing. However the real problem with this argument is that the claims do no support the framework of anonymity at least with respect to how the arguments attempt to distinguish the claims from the prior art. Applicant argues that the anonymity of Wheeler is destroyed because the public key is linked the device. However, turning this logic at the claims yields the same outcome. A record of personal information is indexed using a pointer in a public key certificate. The certificate is contains the public key and the pointer. Therefore the pointer is intrinsically linked to the public key. The public key is tied to the private key which is in and registered to the personal storage device. The personal storage device is associated with the registered user. Thus the index can be traced all the way to the user and device. The notion of anonymity is destroyed by this analysis. The claims need a narrow definition of anonymous and supporting framework to show how the anonymity is preserved during the indexing. There are implied entities other than the user and the device which if expressly defined could support the idea of anonymity with respect to who would know the user or device if accessing the personal records with the certificate. The entity which holds the electronic record system can presumably track the pointer all the way to user. Even the idea of indexing is so broad that it cannot be inferred who is attempting to access the record system. Assuming the record system can trace a record to the user and the user obviously knows his/herself, who is accessing the record which is not supposed to know the user? Applicant mentions removing links between the user and the personal identification contained in the electronic record system but the claim language preserves a link from the user to the information. Thus the claims' anonymous indexing is not anonymous at all. In view of the forgoing, the rejection to independent claim 15 must be maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 115 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2003/0101344 to Wheeler et al., hereinafter Wheeler.

As per claim 115, Wheeler teaches a portable storage device for a registered user of an anonymously indexed electronic record system (0017), the portable storage device being provided with information [PIN} for associating the registered user with the portable storage device (0017, 0138), wherein an asymmetric cryptographic private key is under the control of the portable storage device (0107), wherein an anonymous public key certificate [security certificate (signed public key; 0117)] is associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key (0121, 0165), and wherein association of anonymously indexed personal information with the user is anonymously verifiable by use of the anonymous public key certificate [anonymously verified because a digital signature is formed by anonymous private key attributed to a device for which there is a database linking the device to the user; 0156].

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 116 and 117 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. As per claim 116, the specification does not support or describe demographic information of the user in the public key certificate. As per claim 117, paragraph 0082 describes a situation wherein doctors may be able to retrieve identifiable information from the records when the patient is unable to enter in their pass-phrase. This is not the situation as described in claim 117. Identifiable indexing is performed when the secret pass-phrase has been entered. Furthermore, the [0082] merely describes information can be obtained in situations where the patient can and cannot enter the pass-phrase. The specification is silent with respect to whether anonymity is preserved in situation.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 96-98, 101-105, 107-110, 112-114, and 116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler in view of USP 6,102,287 to Matyas.

As per claim 96, Wheeler teaches a method for anonymously indexing an electronic record system, the method comprising:

storing an asymmetric cryptographic private key within, and under the control of a portable storage device associated with [earmarked to customers] a registered user (0107 and 0133) the private key operating within a public key infrastructure (0104);

creating an anonymous public key certificate [security certificate is digitally signed by a trusted party to authentication the device's public key; 0112, 0117, and Fig. 7] and storing it within the public key infrastructure (0131), the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key [0112, 0122 shows the certificate is linked to the public key which is in turn linked to the private key (0107); 0156 shows that the keys are certificate are all created anonymously and are tied to a device, not a user];

providing the portable storage device with information [PIN] for associating the registered user with the portable storage device (0102 and 0138); and

indexing within an electronic record system personal information of the registered user (0140), whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate [anonymously verified because a digital signature is formed by anonymous private key attributed to a device for which there is a database linking the device to the user; 0142, 0156]. Wheeler is silent in explicitly disclosing wherein the public key certificate containing an electronic report pointer, the electronic record pointer being associated with each item of personal information of the registered user held in the electronic record system and using the electronic record pointer in combination with the anonymous public key certificate to affect anonymous indexing of the personal information. Wheeler does teach personal information including an account number associated with each customer and the database can be indexed using the unique account number (0132-133). Thus an account number acts as a pointer. Matyas teaches a public key certificate that possesses an account number binding the account number to the public key (col. 7, lines 10-25). Account numbers are one known way to anonymously refer to a person. Wheeler already uses the account number to index the database record. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results. Incorporating the account number into a public key certificate was known at the time of the invention. Sending a signed message with the account number as opposed to the personal information still preserves anonymity between the user of the device and an outside party. Thus this modification can be performed without departing from the anonymous framework of Wheeler. Just as using the public key of the device maintained anonymity to the user, an account number just points to the user's files without divulging information about a user to an outside party.

As per claim 103, Wheeler teaches an anonymously indexed electronic record system comprising:

An electronic storage for indexing personal information of a registered user; (0131-0132) and

a portable storage device for a registered user (0107), an asymmetric cryptographic private key being within and under the control of the portable storage device (0112, 0133), the portable storage device being provided with information for associating the registered user with the portable storage device (0107);

and the portable storage device storing an anonymous public key certificate [security certificate; 0165] associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key (0112),

wherein association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate [anonymously verified because a digital signature is formed by anonymous private key attributed to a device for which there is a database linking the device to the user; 0156].

Wheeler is silent in explicitly disclosing wherein the public key certificate containing an electronic report pointer, the electronic record pointer being associated with each item of personal information of the registered user held in the electronic record system and using the electronic record pointer in combination with the anonymous public key certificate to affect anonymous indexing of the personal information. Wheeler does teach personal information including an account number associated with each customer and the database can be indexed using the unique account number (0132-133). Thus an account number acts as a pointer. Matyas teaches a public key certificate that possesses an account number binding the account number to the public key (col. 7, lines 10-25). Account numbers are one known way to anonymously refer to a person. Wheeler already uses the account number to index the database record. The claim is obvious because one of ordinary skill in the art can combine known methods which produce predictable results. Incorporating the account number into a public key certificate was known at the time of the invention. Sending a signed message with the account number as opposed to the personal information still preserves anonymity between the user of the device and an outside party. Thus this modification can be performed without departing from the anonymous framework of Wheeler. Just as using the public key of the device maintained anonymity to the user, an account number just points to the user’s files without divulging information about a user to an outside party.

As per claims 97 and 104, Wheeler teaches the information for associating the registered user with the portable storage device is at least one of: human readable information; and machine readable information (0102).

As per claims 98 and 105, Wheeler teaches the portable storage device is at least one of: a smartcard; and an electronic passport (0100).

As per claims 101 and 107, Wheeler teaches digital signature codes verifiable by using the anonymous public key certificate are created for new data items written into the electronic record system in order to explicitly link each digitally signed data item to the value of the electronic record pointer associated with the digital signature codes [the digital signature is intrinsically linked to the public key and therefore the associated database and its records; 0156] contained within the anonymous public key certificate, and wherein each digital signature code is interpreted as explicitly recording the consent of the registered person associated with the record pointer to the creation of each respective digitally signed data item [inherent that the use of the private key to sign a message is consent of the user who securely and uniquely possesses said private key; 0170].

.

As per claims 102 and 108, Wheeler teaches digital signature codes are created for given data items in the electronic record system using an asymmetric cryptographic private key issued to the registered person, where each digital signature code is interpreted as explicitly recording the consent of the registered person to the creation of each respective digitally signed data item [the digital signature is intrinsically linked to the public key and therefore the associated database and its records; 0156].

As per claim 109, Wheeler teaches the anonymous public key certificate [security certificate; 0165] contains a personal data component [security profile; 0017].

As per claim 110, Wheeler teaches the personal data component comprises biometric data of the registered user (0102).

As per claim 112, Wheeler teaches an access code is stored in the portable storage device allowing access to the asymmetric cryptographic private key (0102).

As per claim 113, Wheeler teaches the asymmetric cryptographic private key can be copied with the registered user's authorization into the possession of an authorized user (0102).

As per claim 114, Wheeler teaches the authorized user is a health care professional authorized by the registered user to enter an update to the registered user's indexed personal information (0132 and 0136).

As per claim 116, Wheeler teaches the anonymous public key certificate held in the personal storage device further comprises data items setting out demographic information of the user (0196).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MICHAEL R VAUGHAN/

Examiner, Art Unit 2431